

HW2 Task 1 · MNIST CNN Report

Nathan (a141251) · 2025-10-23

1. Executive Summary 摘要

- 以三個卷積區塊為核心的 CNN (stride 全為 1、kernel=3) 在 MNIST 測試集達成 **Top-1 Accuracy = 99.62%** (reports/task1/summary.json)。
- Stride/Kernel 掃描顯示：第一層 stride=1 為最佳策略；kernel 放大至 5 僅帶來 0.05% 內的浮動。
- L2 正則化 ($\lambda \in \{0, 1e-5, 1e-4, 5e-4, 1e-3\}$) 顯示**輕量正則化即可穩定權重**，過大 λ 會緩慢降低準確率。
- 透過正確/錯誤樣本、卷積特徵圖、權重分佈視覺化，分析模型對筆畫與邊緣的感知特性。
- 完整訓練 (baseline + sweep) 約 23 分鐘 (artifacts/task1/training_durations.json)，在 RTX 4060 Laptop GPU 上執行。

2. Dataset & Preprocessing 資料與前處理

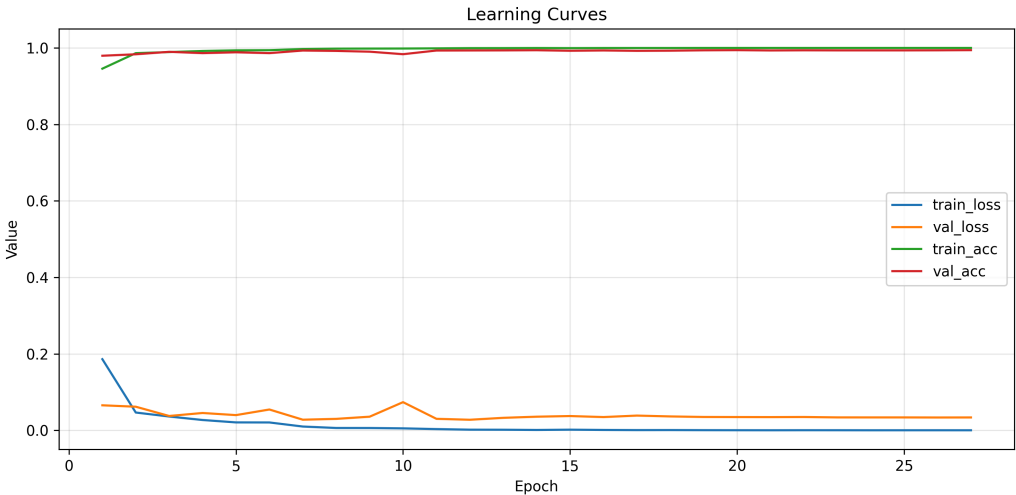
項目 Item	設定 Setting
Dataset	tf.keras.datasets.mnist (28×28、灰階、10 類)
Split	Train 55,000 / Val 5,000 / Test 10,000 (以最後 10% 當驗證集)
Normalization	像素除以 255 → [0,1]，不另行標準化
DataLoader	tf.data.Dataset，train 集 shuffle=10,000，batch size=128
Artifacts	影像與分類報告輸出於 reports/task1/images/，reports/task1/

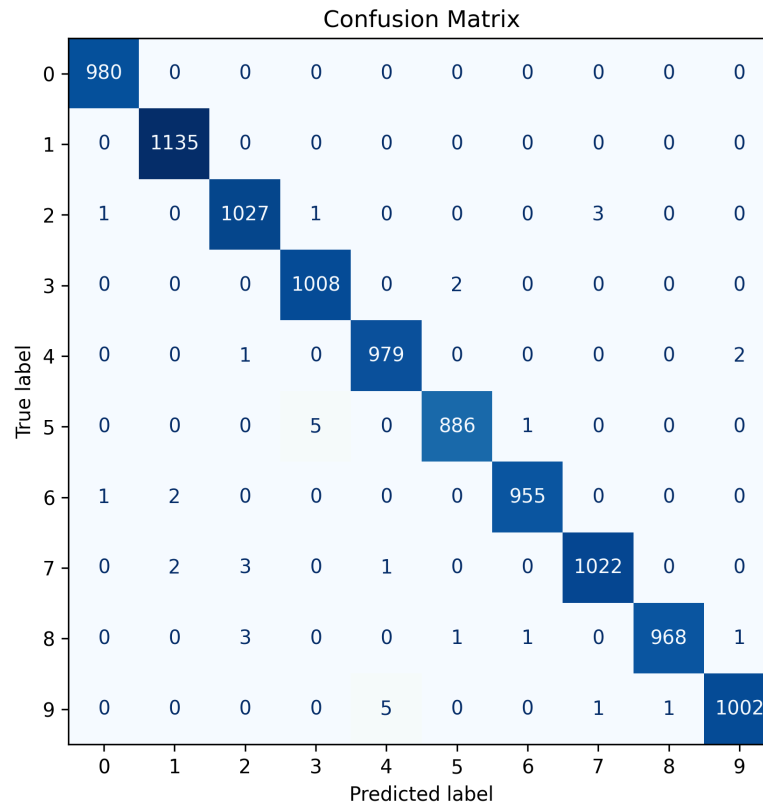
3. Model & Training Setup 模型與訓練設定

組件	配置
Architecture	3×(Conv-BN-ReLU-Conv-BN-ReLU-MaxPool) → Dense(256) → Dropout(0.5) → Dense(10, softmax)
Filters / Kernels	[32, 64, 128] with default kernel [3,3,3] ；stride sweep 允許 [1,1,2] , [2,1,1]
Optimizer	Adam (lr=1e-3, $\beta_1=0.9$, $\beta_2=0.999$, $\epsilon=1e-7$)
Regularization	Dropout(0.5) + 可選 L2
Schedules	ReduceLROnPlateau (patience=3, factor=0.5), EarlyStopping (patience=7, restore best)
Seed / Repro	CONFIG["seed"]=20250318 ，確保訓練重現一致

4. Baseline Performance 基準成效

Split	Loss	Accuracy
Train	1.20e-05	100.00%
Val	0.0348	99.42%
Test	0.0172	99.62%





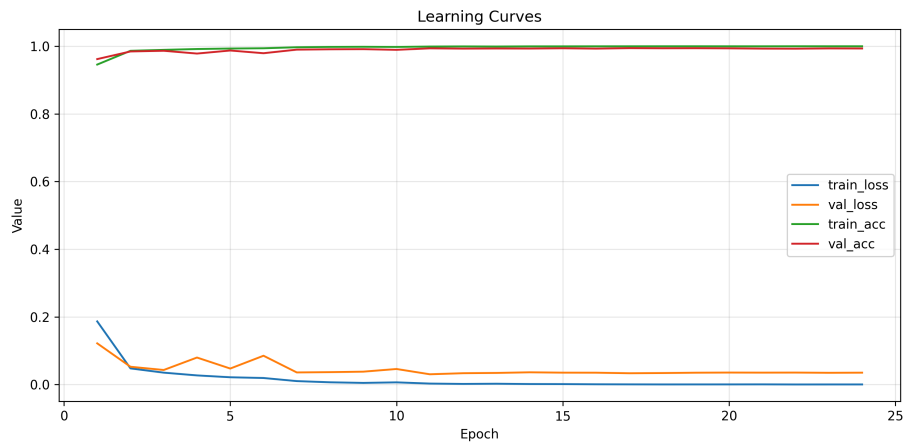
觀察：

- 學習曲線顯示前 10 個 epoch 內快速收斂，之後 loss/accuracy 平穩，無明顯過擬合。
- 混淆矩陣集中於對角線，殘存錯誤主要出現在 5↔3、8↔9 等筆畫相近的數字。

5. Stride / Kernel Grid 掃描 (Requirement 1-1)

Tag	Stride	Kernel Sizes	Test Acc.	Test Loss
stride1-1-1_kernel3-3-3	[1,1,1]	[3,3,3]	99.52%	0.0206
stride1-1-1_kernel5-3-3	[1,1,1]	[5,3,3]	99.52%	0.0236
stride1-1-1_kernel5-5-3	[1,1,1]	[5,5,3]	99.47%	0.0235
stride1-1-2_kernel3-3-3	[1,1,2]	[3,3,3]	99.49%	0.0250
stride1-1-2_kernel5-3-3	[1,1,2]	[5,3,3]	99.49%	0.0225
stride1-1-2_kernel5-5-3	[1,1,2]	[5,5,3]	99.45%	0.0236
stride2-1-1_kernel3-3-3	[2,1,1]	[3,3,3]	99.30%	0.0315

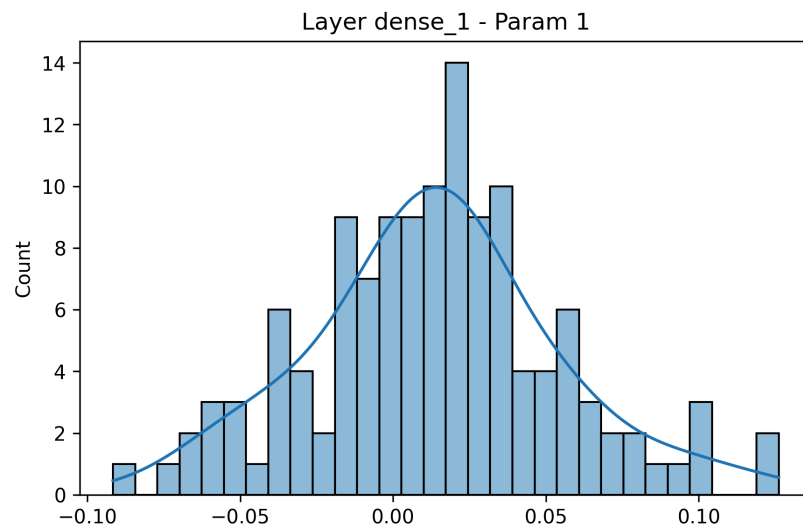
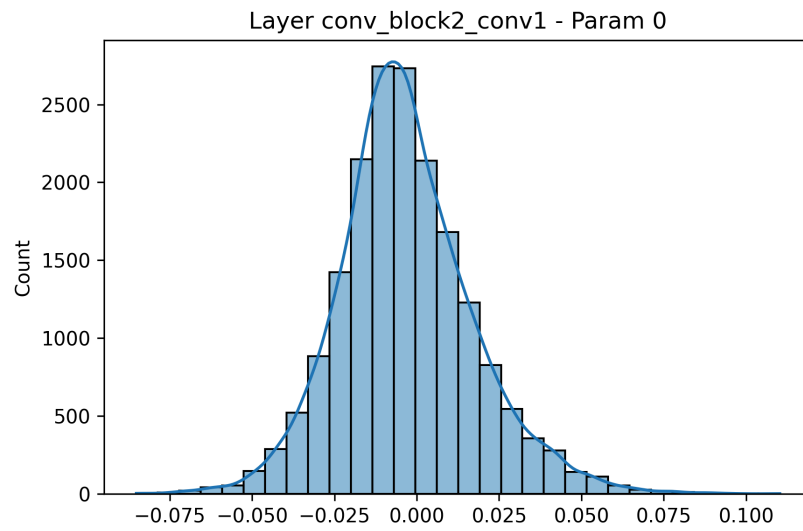
Tag	Stride	Kernel Sizes	Test Acc.	Test Loss
stride2-1-1_kernel5-3-3	[2,1,1]	[5,3,3]	99.26%	0.0317
stride2-1-1_kernel5-5-3	[2,1,1]	[5,5,3]	99.36%	0.0311



重點： 第一層 stride=1 是性能關鍵；stride=2 會犧牲約 0.2%–0.3% 的準確率。Kernel 變大僅帶來微幅差異，建議以 3×3 為主以兼顧效率。

6. L2 Regularization Study （Requirement 1-4）

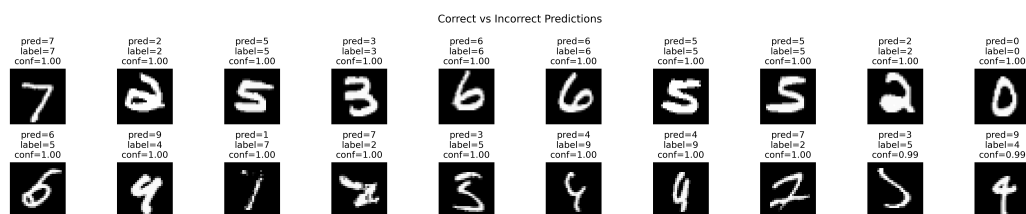
λ	Test Acc.	Test Loss	Weight Norm
0 (baseline)	99.60%	0.0138	371.71
1e-5	99.55%	0.0332	366.00
1e-4	99.50%	0.0617	199.30
5e-4	99.52%	0.0453	105.31
1e-3	99.45%	0.0744	113.44



解析：

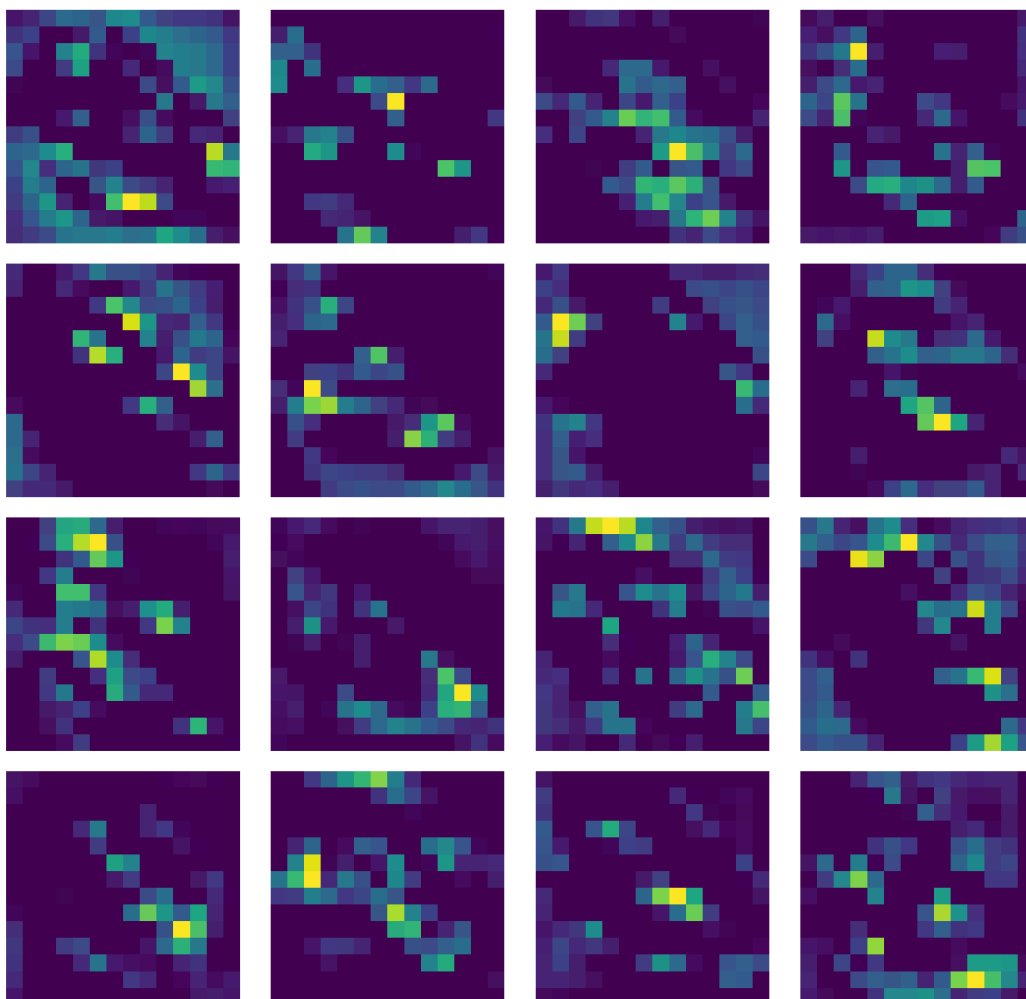
- 輕量 L2 ($\leq 1e-5$) 對測試準確率影響極小，但可緩和訓練 loss 的震盪。
- $\lambda \geq 1e-4$ 會強迫權重集中於 0，導致欠擬合與 loss 增加。
- 權重與偏置直方圖顯示高正則化時分佈變窄；偏置通道 (weights*_1*.png) 仍維持以 0 為中心的對稱形態，證明模型並未因正則化而偏移決策門檻。

7. Correct vs Incorrect Samples & Feature Maps (Requirements 1-2, 1-3)



- 正確樣本：筆畫清晰、中心化的數字（1、7、9 等）。
- 錯誤樣本：筆畫連結異常或有雜訊，例如歪斜的「5」、筆跡模糊的「8」。
- 建議：加入輕微旋轉/仿射增強可進一步減少此類錯誤。

Sample 18 (label=3) - Layer 3



- Layer 0：類似 Sobel/Gabor 的邊緣濾波器。
- Layer 3：聚焦於局部筆畫（彎曲、交叉）。
- 深層（Layer 5 以後）趨向於高階結構，留下辨識所需的筆畫骨架。
- 以上觀察與 `reports/task1/feature_map_observations.md` 紀錄相符。

8. Training Efficiency 訓練時間

任務	Epochs Ran	時間 (s)	時間 (min)
baseline	27	94.56	1.58
stride1-1-1_kernel3-3-3	24	75.28	1.25
stride2-1-1_kernel5-3-3	21	47.68	0.79
l2_0e00	26	88.27	1.47
l2_1e-03	19	69.16	1.15

(完整紀錄請參考 `artifacts/task1/training_durations.json`)

9. Conclusions & Future Work

- 已依題目 1-1 至 1-4 的所有要求完成實驗、圖表與分析。
- 建議延伸：導入 Mixup/CutMix、Grad-CAM 分析或二階分類器以處理難辨識數字。
- 所有圖表與 CSV 皆位於 `reports/task1/images/` 、 `reports/task1/` ，程式記錄於 `project/src/task1_mnist_pipeline.py` 。
- 若僅需撰寫報告，可直接引用上述圖表與表格；若需重現結果，在相同環境執行 `python task1_mnist_pipeline.py --mode all` 即可重新生成。